

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11205305 A**

(43) Date of publication of application: **30 . 07 . 99**

(51) Int. Cl

**H04L 9/32
G06F 15/00
H04L 9/10**

(21) Application number: **10004030**

(71) Applicant: **SONY CORP**

(22) Date of filing: **12 . 01 . 98**

(72) Inventor: **KOMURO TERUYOSHI
OSAWA YOSHITOMO
ASANO TOMOYUKI**

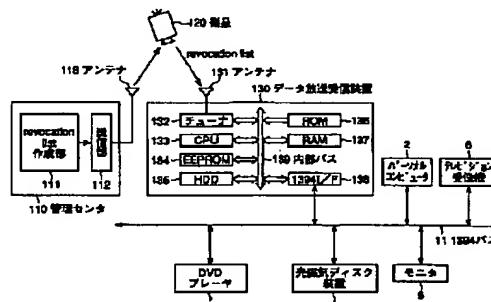
**(54) INFORMATION PROCESSING UNIT AND
METHOD, INFORMATION PROCESSING SYSTEM
AND SERVING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent illegal copying of data by using an illegal device.

SOLUTION: A management center 110 generates a revocation list that describes a device_ID of a device in which information to be kept secret is exposed and sends the generated revocation list to a data broadcast receiver 130 via, e.g. a satellite 120. When the revocation list has been received from the management center 110, the data broadcast receiver 130 compares the device_ID indicated in a received revocation list with a device_ID described in the revocation list in a CDT(connected device_ID table). In the case a device_ID being coincident with the device_ID described in the revocation list in the CDT is detected, the device connected via a 1394 bus 11 is informed of the device_ID.

COPYRIGHT: (C)1999,JPO



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-205305

(43)公開日 平成11年(1999)7月30日

(51)Int.Cl.⁶
H 04 L 9/32
G 06 F 15/00
H 04 L 9/10

識別記号
330

F I
H 04 L 9/00
G 06 F 15/00
H 04 L 9/00

673B
330A
621Z
675D

審査請求 未請求 請求項の数17 O L (全 20 頁)

(21)出願番号 特願平10-4030
(22)出願日 平成10年(1998)1月12日

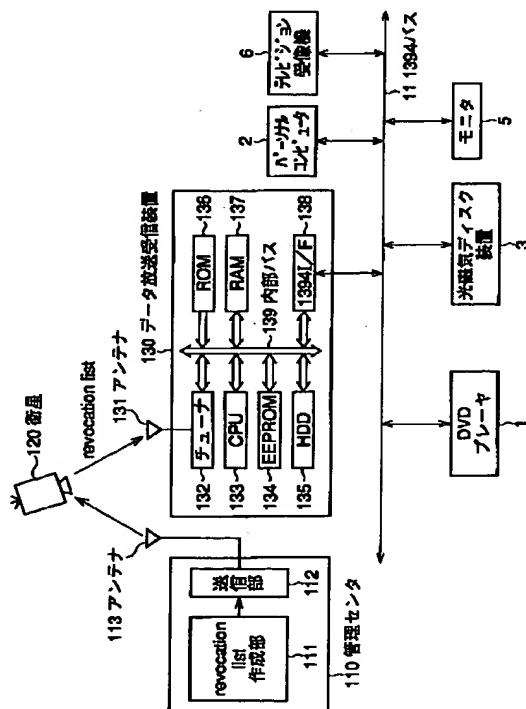
(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72)発明者 小室 輝芳
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72)発明者 大澤 義知
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(74)代理人 弁理士 稲本 義雄

(54)【発明の名称】 情報処理装置および方法、情報処理システム、並びに提供媒体

(57)【要約】

【課題】 不正装置によるデータの不正コピーを防止す
る。

【解決手段】 管理センタ110は、秘密裡にしておくべき情報が露呈された装置のdevice_IDを記したリボケーションリストを作成し、作成したリボケーションリストを、例えば、衛星120を介して、データ放送受信装置130に提供する。データ放送受信装置130は、管理センタ110からリボケーションリストが提供された場合、受信されたリボケーションリストに示されているdevice_IDと、CDT (connected device_ID table) 中に格納しているdevice_IDとを比較し、CDT中に、リボケーションリストに記されているdevice_IDと合致するdevice_IDが存在したとき、そのdevice_IDを、1394バス11を介して接続されてる装置に知らせる。



【特許請求の範囲】

【請求項1】 他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成手段と、前記作成手段により作成された前記リストを、前記他の情報処理装置のうち、前記第1の情報処理装置以外の第2の情報処理装置に提供する提供手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記作成手段により作成された前記リストに、自分自身のデジタル署名を付加する付加手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項3】 前記付加手段は、さらに、前記リストが作成された時刻を付加することを特徴とする請求項2に記載の情報処理装置。

【請求項4】 他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成ステップと、前記作成ステップで作成された前記リストを、前記他の情報処理装置のうち、前記第1の情報処理装置以外の第2の情報処理装置に提供する提供ステップとを備えることを特徴とする情報処理方法。

【請求項5】 他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成ステップと、前記作成ステップで作成された前記リストを、前記他の情報処理装置のうち、前記第1の情報処理装置以外の第2の情報処理装置に提供する提供ステップとを有するコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項6】 所定の伝送路を介して接続されている他の情報処理装置に暗号化データを伝送する情報処理装置において、

前記他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信手段と、前記受信手段により受信された前記リストに記されている前記識別番号と、前記記憶手段により記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段による比較結果に対応して、前記暗号化データを前記他の情報処理装置に伝送する伝送手段とを備えることを特徴とする情報処理装置。

【請求項7】 前記情報は、暗号化されているデータを復号するための鍵であることを特徴とする請求項6に記載の情報処理装置。

【請求項8】 前記リストには、前記リストを作成した装置の署名が与えられており、前記リストに付加されている前記署名を用いて、前記リ

ストが正規のものであるか否かを検証する検証手段をさらに備えることを特徴とする請求項6に記載の情報処理装置。

【請求項9】 前記比較手段による比較の結果、前記リスト中の識別番号と合致する識別番号が前記識別番号テーブル中に存在した場合、前記識別番号テーブル中の、対応する前記識別番号にフラグを付加する付加手段をさらに備えることを特徴とする請求項6に記載の情報処理装置。

10 【請求項10】 前記伝送手段は、接続されている前記他の情報処理装置のうち、前記付加手段により前記フラグが付加された前記識別番号に対応する情報処理装置には、前記暗号化データまたは前記暗号化データを復号するための鍵をを伝送しないことを特徴とする請求項9に記載の情報処理装置。

【請求項11】 前記伝送手段は、さらに、前記付加手段により前記フラグが付加された前記識別番号を含む前記識別番号テーブルを、前記他の情報処理装置に伝送することを特徴とする請求項9に記載の情報処理装置。

20 【請求項12】 前記伝送路は、IEEE1394バスであることを特徴とする請求項6に記載の情報処理装置。

【請求項13】 所定の伝送路を介して接続されている他の情報処理装置に暗号化データを伝送する情報処理装置における情報処理方法において、前記他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信手段と、

30 前記受信手段で受信された前記リストに記されている前記識別番号と、前記記憶手段で記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段における比較結果に対応して、前記暗号化データを前記他の情報処理装置に伝送する伝送手段とを備えることを特徴とする情報処理方法。

【請求項14】 所定の伝送路を介して接続されている他の情報処理装置に暗号化データを伝送する情報処理装置に用いられるコンピュータプログラムを提供する提供媒体において、

前記他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、

秘密裡に保管しておくべき情報が露呈された装置の識別番号が記されたリストを受信する受信手段と、前記受信手段で受信された前記リストに記されている前記識別番号と、前記記憶手段で記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段における比較結果に対応して、前記暗号化データを前記他の情報処理装置に伝送する伝送手段

ップとを有するコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項15】 第1の情報処理装置乃至第3の情報処理装置により構成される情報処理システムにおいて、前記第1の情報処理装置は、

秘密裡にしておくべき情報が露呈された前記第3の情報処理装置の識別番号を示したリストを作成する作成手段と、

前記作成手段により作成された前記リストを前記第2の情報処理装置に提供する提供手段とを備え、

前記第2の情報処理装置は、

所定の伝送路を介して接続されている前記第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、

前記第1の情報処理装置の前記提供手段により提供された前記リストを受信する受信手段と、

前記受信手段により受信された前記リストに示されている前記識別番号と、前記記憶手段により記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段による比較結果に対応して、前記第3の情報処理装置に暗号化データを伝送する伝送手段とを備えることを特徴とする情報処理システム。

【請求項16】 第1の情報処理装置乃至第3の情報処理装置により構成される情報処理システムにおける情報処理方法において、

前記第1の情報処理装置は、

秘密裡にておくべき情報が露呈された前記第3の情報処理装置の識別番号を示したリストを作成する作成手段と、

前記作成手段により作成された前記リストを前記第2の情報処理装置に提供する提供手段とを備え、

前記第2の情報処理装置は、

所定の伝送路を介して接続されている前記第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、

前記第1の情報処理装置の前記提供手段により提供された前記リストを受信する受信手段と、

前記受信手段により受信された前記リストに示されている前記識別番号と、前記記憶手段により記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段による比較結果に対応して、前記第3の情報処理装置に暗号化データを伝送する伝送手段とを備えることを特徴とする情報処理方法。

【請求項17】 第1の情報処理装置乃至第3の情報処理装置により構成される情報処理システムに用いられるコンピュータプログラムを提供する提供媒体において、前記第1の情報処理装置は、

秘密裡にておくべき情報が露呈された前記第3の情報

処理装置の識別番号を示したリストを作成する作成手段と、

前記作成手段により作成された前記リストを前記第2の情報処理装置に提供する提供手段とを備え、

前記第2の情報処理装置は、

所定の伝送路を介して接続されている前記第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、

前記第1の情報処理装置の前記提供手段により提供された前記リストを受信する受信手段と、

前記受信手段により受信された前記リストに示されている前記識別番号と、前記記憶手段により記憶された前記識別番号テーブル中の前記識別番号とを比較する比較手段と、

前記比較手段による比較結果に対応して、前記第3の情報処理装置に暗号化データを伝送する伝送手段とを有するコンピュータプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理装置および方法、情報処理システム、並びに提供媒体に関し、特に、不正装置によるデータの不正コピーを防止することができるようとした、情報処理装置および方法、情報処理システム、並びに提供媒体に関する。

【0002】

【従来の技術】 最近、AV機器やパーソナルコンピュータなどの電子機器を、例えばIEEE1394バス（以下、単に1394バスと称する）などの伝送路を介して相互に接続し、相互の間でデータを授受することができるようするシステムが提案されている。

【0003】 図9は、そのような情報処理システムの構成例を示している。なお、本明細書において、システムとは、複数の装置で構成される全体的な装置を示すものとする。この例においては、1394バス11を介してDVD（Digital Video Disk）プレーヤ1、パーソナルコンピュータ2、光磁気ディスク装置3、データ放送受信装置4、モニタ5、テレビジョン受像機6が相互に接続されている。

【0004】

図10は、この内のDVDプレーヤ1、パーソナルコンピュータ2、および光磁気ディスク装置3の内部のより詳細な構成例を表している。DVDプレーヤ1は、1394インターフェース（I/F）26を介して、1394バス11に接続されている。CPU21は、ROM22に記憶されているプログラムに従って各種の処理を実行し、RAM23は、CPU21が各種の処理を実行する上において必要なデータやプログラムなどを適宜記憶する。操作部24は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより操作されたとき、その操作に対応する信号を出力する。ドライブ25は、図示せぬ

DVD（ディスク）を駆動し、そこに記録されているデータを再生するようになされている。EEPROM (electricaly erasable programmable ROM) 27は、装置の電源オフ後も記憶する必要のある情報を記憶するようになされている。内部バス28は、これらの各部を相互に接続している。

【0005】光磁気ディスク装置3は、CPU31乃至内部バス38を有している。これらは、上述したDVDプレーヤ1におけるCPU21乃至内部バス28と同様の機能を有するものであり、その説明は省略する。ただし、ドライブ35は、図示せぬ光磁気ディスクを駆動し、そこにデータを記録または再生するようになされている。

【0006】パーソナルコンピュータ2は、1394インターフェース49を介して1394バス11に接続されている。CPU41は、ROM42に記憶されているプログラムに従つて各種の処理を実行する。RAM43には、CPU41が各種の処理を実行する上において必要なデータやプログラムなどが適宜記憶される。入出力インターフェース44は、キーボード45とマウス46が接続されており、それらから入力された信号をCPU41に出力するようになされている。また、入出力インターフェース44には、ハードディスク（HDD）47が接続されており、CPU41は、そこにデータ、プログラムなどを記録再生させることができるようになされている。入出力インターフェース44にはまた、拡張ボード48を適宜装着し、必要な機能を附加することができるようになされている。EEPROM50には、電源オフ後も保持する必要のある情報が記憶されるようになされている。例えば、PCI(Peripheral Component Interconnect)、ローカルバスなどにより構成される内部バス51は、これらの各部を相互に接続するようになされている。

【0007】なお、この内部バス51は、ユーザに対して解放されており、ユーザは、拡張ボード48に所定のボードを適宜接続したり、所定のソフトウェアプログラムを作成して、CPU41にインストールすることで、内部バス51により伝送されるデータを適宜受信することができるようになされている。

【0008】これに対して、DVDプレーヤ1や光磁気ディスク装置3などのコンシューマエレクトロニクス（CE）装置においては、内部バス28や内部バス38は、ユーザに解放されておらず、特殊な改造などを行わない限り、そこに伝送されるデータを取得することができないようになされている。

【0009】以上の構成のシステムにおいて、例えば、ユーザが、DVDに記録されている映画を、モニタ5またはテレビジョン受像器6等の表示装置を用いて観賞する場合、DVDプレーヤ1は、DVD（ディスク）から読みとった映画データを、1394バス11を介して表示装置に伝送し、表示装置は、それを受信して表示する。

【0010】ところで、このとき、映画データをそのま

まの状態で1394バス11を介して伝送すると、不正なユーザがその映画データを受信し、それを不法コピーする可能性がある。そこで、送信側の装置（以下、このような装置をソース（source）と称する）は伝送するデータを暗号化して伝送し、受信側の装置（以下、このような装置をシンク（sink）と称する）は、それを鍵を用いて復号するようにする。その際、送信側の装置は、相手の装置が正規の装置であるか否かを判断するために、データを伝送する前に、その装置との間で認証処理を実行する。

【0011】以下に、ソースとシンクとの間で行われる認証処理について説明する。この認証処理は、図11に示すように、ソースとしての、例えばDVDプレーヤ1のROM22に予め記憶されているソフトウェアプログラムの1つとしてのファームウェア20と、シンクとしての、例えばパーソナルコンピュータ2のROM42に記憶されており、CPU41が処理するソフトウェアプログラムの1つとしてのライセンスマネージャ62との間において行われる。

【0012】図12は、ソース（DVDプレーヤ1）と、シンク（パーソナルコンピュータ2）との間において行われる認証の手順を示している。DVDプレーヤ1のEEPROM27には、サービスキー（service_key）と関数（hash）が予め記憶されている。これらはいずれも伝送するデータ（映画データ）の著作権者から、このDVDプレーヤ1のユーザに与えられたものであり、各ユーザは、EEPROM27に、これを秘密裡に保管しておくものである。

【0013】サービスキーは、著作権者が提供する情報毎に与えられるものであり、この1394バス11で構成されるシステムにおいて、共通のものである。hash関数は、任意長の入力に対して、64ビットまたは128ビットなどの固定長のデータを出力する関数であり、 $y (=hash(x))$ を与えたとき、 x を求めることが困難であり、かつ、 $hash(x_1)=hash(x_2)$ となる x_1 と、 x_2 の組を求めることが困難となる関数である。1方向hash関数の代表的なものとして、MD5やSHAなどが知られている。この1方向hash関数については、Bruce Schneier著の「Applied Cryptography (Second Edition), Wiley」に詳しく解説されている。

【0014】一方、シンクとしての例えばパーソナルコンピュータ2は、著作権者から与えられた、自分自身に固有の識別番号（device_ID：以下、適宜、IDと略記する）とライセンスキーキー（license_key）を、EEPROM50に秘密裡に保持している。このライセンスキーキーは、nビットのIDとmビットのサービスキーを連結して得たn+mビットのデータ（ID || service_key）に対して、hash関数を適用して得られる値である。すなわち、ライセンスキーキーは次式で表される。 $licence_key=hash(ID || service_key)$

【0015】IDとしては、例えば1394バス11の規格に

定められているnode_unique_IDを用いることができる。このnode_unique_IDは、図12に示すように、8バイト(64ビット)で構成され、最初の3バイトは、IEEEで管理され、電子機器の各メーカーにIEEEから付与される。また、下位5バイトは、各メーカーが、自分自身がユーザに提供する各装置に対して付与することができるものである。各メーカーは、例えば下位5バイトに対してシリアルに、1台に1個の番号を割り当てるようにし、5バイト分を全部使用した場合には、上位3バイトがさらに別の番号となっているnode_unique_IDの付与を受け、そして、その下位5バイトについて1台に1個の番号を割り当てるようになる。従って、このnode_unique_IDは、メーカーに拘らず、1台毎に異なるものとなり、各装置に固有のものとなる。

【0016】まず、ステップS1において、DVDプレーヤ1のファームウェア20は、1394インターフェース26を制御し、1394バス11を介してパーソナルコンピュータ2に対してIDを要求する。パーソナルコンピュータ2のライセンスマネージャ62は、ステップS2において、このIDの要求を受信する。すなわち、1394インターフェース49は、1394バス11を介してDVDプレーヤ1から伝送されてきたID要求の信号を受信すると、これをCPU41に出力する。CPU41のライセンスマネージャ62は、このID要求を受けたとき、ステップS3においてEEPROM50に記憶されているIDを読み出し、これを1394インターフェース49を介して1394バス11からDVDプレーヤ1に伝送する。

【0017】DVDプレーヤ1においては、ステップS4で、1394インターフェース26がパーソナルコンピュータ2から伝送されたIDを受け取ると、このIDはCPU21で動作しているファームウェア20に供給される。

【0018】ファームウェア20は、ステップS5において、パーソナルコンピュータ2から伝送を受けたIDと、EEPROM27に記憶されているサービスキーを連結して、連結データ(ID || service_key)を生成し、このデータに対して、次式に示すようにhash関数を適用して、キーlkを生成する。

$$lk = \text{hash}(\text{ID} \parallel \text{service_key})$$

【0019】次に、ステップS6において、ファームウェア20は、暗号鍵skを生成する。この暗号鍵skは、セッションキーとしてDVDプレーヤ1とパーソナルコンピュータ2のそれぞれにおいて共通に利用される。

【0020】次に、ステップS7において、ファームウェア20は、ステップS5で生成した鍵lkを鍵として用いて、ステップS6で生成した暗号鍵skを暗号化することにより、暗号化データ(暗号化鍵)eを得る。すなわち、次式を演算する。なお、Enc(A, B)は、共通鍵暗号方式で、鍵Aを用いて、データBを暗号化することを意味する。

$$e = \text{Enc}(lk, sk)$$

【0021】次に、ステップS8で、ファームウェア20は、ステップS7で生成した暗号化データeをパーソナルコンピュータ2に伝送する。すなわち、この暗号化データeは、DVDプレーヤ1の1394インターフェース26から1394バス11を介してパーソナルコンピュータ2に伝送される。パーソナルコンピュータ2においては、ステップS9で、この暗号化データeを1394インターフェース49を介して受信する。ライセンスマネージャ62は、このようにして受信した暗号化データeをEEPROM50に記憶されているライセンスキーを鍵として用いて、次式に示すように復号し、復号鍵sk'を生成する。なお、ここで、Dec(A, B)は、共通鍵暗号方式で鍵Aを用いて、データBを復号することを意味する。

$$sk' = \text{Dec}(\text{license_key}, e)$$

【0022】なお、この共通鍵暗号方式における暗号化的アルゴリズムとしては、DES(Data Encryption Standard:米国データ暗号化規格)が知られている。共通鍵暗号方式についても、上述した、Applied Cryptography(Second Edition)に詳しく解説されている。

【0023】DVDプレーヤ1において、ステップS5で生成するキーlkは、パーソナルコンピュータ2のEEPROM50に記憶されている(license_key)と同一の値となる。すなわち、次式が成立する。

$$lk = \text{license_key}$$

【0024】従って、パーソナルコンピュータ2において、ステップS10で復号して得たキーsk'は、DVDプレーヤ1において、ステップS6で生成した暗号鍵skと同一の値となる。すなわち、次式が成立する。

$$sk' = sk$$

【0025】このように、DVDプレーヤ1(ソース)とパーソナルコンピュータ2(シンク)の両方において、同一の鍵sk, sk'を共有することができる。そこで、この鍵skをそのまま暗号鍵として用いるか、あるいは、これを基にして、それぞれが疑似乱数を作り出し、それを暗号鍵として用いることができる。

【0026】ライセンスキーは、上述したように、各装置に固有のIDと、提供する情報に対応するサービスキーに基づいて生成されているので、他の装置がskまたはsk'を生成することはできない。また、著作権者から認められていない装置は、ライセンスキーを有していないので、skあるいはsk'を生成することができない。従つて、その後DVDプレーヤ1が暗号鍵skを用いて再生データを暗号化してパーソナルコンピュータ2に伝送した場合、パーソナルコンピュータ2が適正にライセンスキーを得たものである場合には、暗号鍵sk'を有しているので、DVDプレーヤ1より伝送されてきた、暗号化されている再生データを復号することができる。しかしながら、パーソナルコンピュータ2が適正なものでない場合、暗号鍵sk'を有していないので、伝送されてきた暗号化されている再生データを復号することができない。

換言すれば、適正な装置だけが共通の暗号鍵sk, sk'を生成することができるので、結果的に、認証が行われることになる。

【0027】仮に1台のパーソナルコンピュータ2のライセンスキーが盗まれたとしても、IDが1台1台異なるので、そのライセンスキーを用いて、他の装置がDVDプレーヤ1から伝送されてきた暗号化されているデータを復号することはできない。従って安全性が向上する。

【0028】ところで、何らかの理由により、不正なユーザが、暗号化データeと暗号鍵skを両方とも知ってしまったような場合のことを考える。この場合、eは、平文skを、鍵1kで暗号化した暗号文であるので、暗号アルゴリズムが公開されている場合、不正ユーザは、鍵1kを総当たりで試すことにより、正しい鍵1kを得る可能性がある。

【0029】不正ユーザによるこの種の攻撃を、より困難にするために、暗号アルゴリズムの一部または全部を一般に公開せずに秘密にしておくことができる。

【0030】または同様に、license_keyから、service_keyを総当たりで調べる攻撃を、より困難にするために、hash関数の一部または全文を一般に公開せずに秘密にしておくようにすることもできる。

【0031】図14は、ソース(DVDプレーヤ1)に対して、パーソナルコンピュータ2だけでなく、光磁気ディスク装置3もシンクとして機能する場合の処理例を表している。

【0032】この場合、シンク1としてのパーソナルコンピュータ2のEEPROM50には、IDとしてID1が、また、ライセンスキーとしてlicense_key1が記憶されており、シンク2としての光磁気ディスク装置3においては、EEPROM37に、IDとしてID2が、また、ライセンスキーとしてlicense_key2が記憶されている。

【0033】DVDプレーヤ1(ソース)とパーソナルコンピュータ2(シンク1)の間において行われるステップS11乃至ステップS20の処理は、図12におけるステップS1乃至ステップS10の処理と実質的に同様の処理であるので、その説明は省略する。

【0034】すなわち、上述したようにして、DVDプレーヤ1は、パーソナルコンピュータ2に対して認証処理を行う。そして次に、ステップS21において、DVDプレーヤ1は、光磁気ディスク装置3に対して、IDを要求する。光磁気ディスク装置3においては、ステップS22で1394インターフェース36を介して、このID要求信号が受信されると、そのファームウェア30(図18)は、ステップS23でEEPROM37に記憶されているID(ID2)を読み出し、これを1394インターフェース36から、1394バス11を介してDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS24で、1394インターフェース26を介して、このID2を受け取ると、ステップS25で、次式から鍵1k2を生成す

る。

$1k2 = \text{hash} (ID2 \parallel \text{service_key})$

【0035】さらに、ファームウェア20は、ステップS26で次式を演算し、ステップS16で生成した鍵skを、ステップS25で生成した鍵1k2を用いて暗号化し、暗号化したデータe2を生成する。 $e2 = \text{Enc} (1k2, sk)$

【0036】そして、ステップS27で、ファームウェア20は、この暗号化データe2を1394インターフェース26から1394バス11を介して光磁気ディスク装置3に伝送する。

【0037】光磁気ディスク装置3においては、ステップS28で、1394インターフェース36を介してこの暗号化データe2を受信し、ステップS29で、次式を演算して暗号鍵sk2'を生成する。

$sk2' = \text{Dec} (\text{license_key}2, e2)$

【0038】以上のようにして、パーソナルコンピュータ2と光磁気ディスク装置3のそれぞれにおいて、暗号鍵sk1', sk2'が得られたことになる。これらの値は、DVDプレーヤ1における暗号鍵skと同一の値となっている。

【0039】図14の処理例においては、DVDプレーヤ1が、パーソナルコンピュータ2と、光磁気ディスク装置3に対して、それぞれ個別にIDを要求し、処理するようになっているのであるが、同報通信によりIDを要求することができる場合は、図14に示すような処理を行うことができる。

【0040】すなわち、図15の処理例においては、ステップS41で、ソースとしてのDVDプレーヤ1が、全てのシンク(この例の場合、パーソナルコンピュータ2と光磁気ディスク装置3)に対して同報通信でIDを要求する。パーソナルコンピュータ2と光磁気ディスク装置3は、それぞれステップS42とステップS43で、このID転送要求の信号を受け取ると、それぞれステップS44またはステップS45で、EEPROM50またはEEPROM37に記憶されているID1またはID2を読み出し、これをDVDプレーヤ1に転送する。DVDプレーヤ1は、ステップS46とステップS47で、これらのIDをそれぞれ受信する。

【0041】DVDプレーヤ1においては、さらにステップS48で、次式から暗号鍵1k1を生成する。

$1k1 = \text{hash} (ID1 \parallel \text{service_key})$

【0042】さらに、ステップS49において、次式から暗号鍵1k2が生成される。

$1k2 = \text{hash} (ID2 \parallel \text{service_key})$

【0043】DVDプレーヤ1においては、さらにステップS50で、暗号鍵skが生成され、ステップS51で、次式で示すように、暗号鍵skが、鍵1k1を鍵として暗号化される。

$e1 = \text{Enc} (1k1, sk)$

【0044】さらに、ステップS52においては、暗号鍵skが、鍵lk2を鍵として、次式に従って暗号化される。

$$e_2 = \text{Enc} (lk_2, sk)$$

【0045】さらに、ステップS53においては、ID1, e1, ID2, e2が、それぞれ次式で示すように連結されて、暗号化データeが生成される。

$$e = ID_1 \parallel e_1 \parallel ID_2 \parallel e_2$$

【0046】DVDプレーヤ1においては、さらにステップS54で、以上のようにして生成された暗号化データeが同報通信で、パーソナルコンピュータ2と光磁気ディスク装置3に伝送される。

【0047】パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS55またはステップS56で、これらの暗号化データeが受信される。そして、パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS57またはステップS58において、次式で示す演算が行われ、暗号鍵sk1', sk2'が生成される。

$$sk_1' = \text{Dec} (\text{license_key } 1, e_1)$$

$$sk_2' = \text{Dec} (\text{license_key } 2, e_2)$$

【0048】図16は、1つのシンクが複数のサービスを受けること（複数の種類の情報の復号）ができるようになされている場合の処理例を表している。すなわち、この場合においては、例えば、シンクとしてのパーソナルコンピュータ2は、複数のライセンスキー（license_key1, license_key2, license_key3など）をEEPROM50に記憶している。ソースとしてのDVDプレーヤ1は、そのEEPROM27に複数のサービスキー（service_key1, service_key2, service_key3など）を記憶している。この場合、DVDプレーヤ1は、ステップS81でシンクとしてのパーソナルコンピュータ2に対してIDを要求するとき、DVDプレーヤ1が、これから転送しようとする情報（サービス）を識別するservice_IDを転送する。パーソナルコンピュータ2においては、ステップS82で、これを受信したとき、EEPROM50に記憶されている複数のライセンスキーの中から、このservice_IDに対応するものを選択し、これを用いて、ステップS90で復号処理を行う。その他の動作は、図11における場合と同様である。

【0049】図17は、さらに他の処理例を表している。この例においては、ソースとしてのDVDプレーヤ1が、そのEEPROM27に、service_key、hash関数、および疑似乱数発生関数pRNGを記憶している。これらは、著作権者から与えられたものであり、秘密裡に保管される。また、シンクとしてのパーソナルコンピュータ2のEEPROM50には、著作権者から与えられたID、LK, LK'、関数G、および疑似乱数発生関数pRNGを有している。

【0050】LKは、著作権者が作成したユニークな乱数

であり、LK'は、次式を満足するように生成されてい

$$LK' = G^{\wedge} - 1 \quad (R)$$

$$R = pRNG (H) \quad (+) \quad pRNG (LK)$$

$$H = \text{hash} (ID \parallel \text{service_key})$$

【0051】なお、G^{\wedge} - 1 (^はべき乗を意味する)は、Gの逆関数を意味する。G^{\wedge} - 1は、所定の規則を知つていれば、簡単に計算することができるが、知らない場合には、計算することが難しいような特徴を有している。このような関数としては、公開鍵暗号に用いられている関数を利用することができる。

【0052】また、疑似乱数発生関数は、ハードウェアとして設けるようにすることも可能である。

【0053】DVDプレーヤ1のファームウェア20は、最初にステップS101において、パーソナルコンピュータ2のライセンスマネージャ62に対してIDを要求する。パーソナルコンピュータ2のライセンスマネージャ62は、ステップS102でID要求信号を受け取ると、EEPROM50に記憶されているIDを読み出し、ステップS

103で、これをDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS104でこのIDを受け取ると、ステップS105で次式を演算する。

$$H = \text{hash} (ID \parallel \text{service_key})$$

【0054】さらに、ファームウェア20は、ステップS106で鍵skを生成し、ステップS107で次式を演算する。

$$e = sk \quad (+) \quad pRNG (H)$$

【0055】なお、A (+) Bは、AとBの排他的論理和の演算を意味する。

【0056】すなわち、疑似ランダム発生キーpRNGにステップS105で求めたHを入力することで得られた結果、pRNG(H)と、ステップS106で生成した鍵skのビット毎の排他的論理和を演算することで、鍵SKを暗号化する。

【0057】次に、ステップS108で、ファームウェア20は、eをパーソナルコンピュータ2に伝送する。

【0058】パーソナルコンピュータ2においては、ステップS109でこれを受信し、ステップS110で、次式を演算する。

$$sk' = e \quad (+) \quad G (LK') \quad (+) \quad pRNG (LK)$$

【0059】すなわち、DVDプレーヤ1から伝送されたe、EEPROM50に記憶されている関数Gに、やはりEEPROM50に記憶されているLK'を適用して得られる値G(LK')、並びに、EEPROM50に記憶されているLK'を、やはりEEPROM50に記憶されている疑似乱数発生関数pRNGに適用して得られる結果pRNG(LK)の排他的論理和を演算し、鍵sk'を得る。

【0060】ここで、次式に示すように、sk=sk'となる。

$$\begin{aligned}
 sk' &= e (+) G (LK') (+) pRNG (LK) \\
 &= sk (+) pRNG (H) (+) R (+) pRNG (LK) \\
 &= sk (+) pRNG (H) (+) pRNG (H) (+) pRNG (LK) (+) \\
) pRNG (LK) \\
 &= sk
 \end{aligned}$$

【0061】このようにして、ソースとしてのDVDプレーヤ1とシンクとしてのパーソナルコンピュータ2は、同一の鍵sk, sk'を共有することができる。LK, LK'を作ることができるのは、著作権者だけであるので、ソースが不正に、LK, LK'を作ろうとしても作ることができないので、より安全性を高めることができる。

【0062】以上においては、ソースとシンクにおいて認証を行うようにしたが、例えばパーソナルコンピュータ2には、通常、任意のアプリケーションプログラムをロードして用いることができる。そして、このアプリケーションプログラムとしては、不正に作成したものが使用される場合もある。従って、各アプリケーションプログラム毎に、著作権者から許可を得たものであるか否かを判定する必要がある。そこで、図12に示すように、各アプリケーション部61とライセンスマネージャ62との間においても、上述したように、認証処理を行うようになることができる。この場合、ライセンスマネージャ62がソースとなり、アプリケーション部61がシンクとなる。

【0063】次に、以上のようにして、認証が行われた後（暗号鍵の共有が行われた後）、暗号鍵を用いて、ソースから暗号化したデータをシンクに転送し、シンクにおいて、この暗号化したデータを復号する場合の動作について説明する。

【0064】図18に示すように、DVDプレーヤ1、あるいは光磁気ディスク装置3のように、内部の機能が一般ユーザーに解放されていない装置においては、1394バス11を介して授受されるデータの暗号化と復号の処理は、それぞれ1394インターフェース26または1394インターフェース36で行われる。この暗号化と復号化には、セッションキーSと時変キーiが用いられるが、このセッションキーSと時変キーi（正確には、時変キーiを生成するためのキーi'）は、それぞれファームウェア20またはファームウェア30から、1394インターフェース26または1394インターフェース36に供給される。セッションキーSは、初期値として用いられる初期値キーSsと時変キーiを攪乱するために用いられる攪乱キーSiにより構成されている。この初期値キーSsと攪乱キーSiは、上述した認証において生成された暗号鍵sk（=sk'）の所定のビット数の上位ビットと下位ビットにより、それぞれ構成するようにすることができる。このセッションキーSは、セッション毎に（例えば、1つの映画情報毎に、あるいは、1回の再生毎に）、適宜、更新される。これに対して、攪乱キーSiとキーi'から生成される時変キーiは、1つのセッション内において、頻

繁に更新されるキーであり、例えば、所定のタイミングにおける時刻情報を用いることができる。

【0065】いま、ソースとしてのDVDプレーヤ1から再生出力した映像データを1394バス11を介して光磁気ディスク装置3とパーソナルコンピュータ2に伝送し、それぞれにおいて復号するものとする。この場合、DVDプレーヤ1においては、1394インターフェース26において、セッションキーSと時変キーiを用いて暗号化処理が行われる。光磁気ディスク装置3においては、1394インターフェース36において、セッションキーSと時変キーiを用いて復号処理が行われる。

【0066】これに対して、パーソナルコンピュータ2においては、ライセンスマネージャ62が、セッションキーSのうち、初期値キーSsをアプリケーション部61に供給し、攪乱キーSiと時変キーi（正確には、時変キーiを生成するためのキーi'）を1394インターフェース49（リンク部分）に供給する。そして、1394インターフェース49において、攪乱キーSiとキーi'から時変キーiが生成され、時変キーiを用いて復号が行われ、その復号されたデータは、アプリケーション部61において、さらにセッションキーS（正確には、初期値キーSs）を用いて復号が行われる。

【0067】このように、パーソナルコンピュータ2においては、内部バス51が、ユーザーに解放されているので、1394インターフェース49により第1段階の復号だけを行い、まだ暗号の状態としておく。そして、アプリケーション部61において、さらに第2段階の復号を行い、平文にする。これにより、パーソナルコンピュータ2に対して、適宜、機能を付加して、内部バス51において授受されるデータ（平文）をハードディスク47や他の装置にコピーすることを禁止させる。

【0068】

【発明が解決しようとする課題】しかしながら、以上のような認証方法を用いても、例えば、所定の装置がリバースエンジニアリング等の何らかの処理が施され、その装置において秘密裡に保管しておくべき情報（例えば、鍵情報）が露呈した（盗まれた）場合、それらの情報を用いて、暗号化データが復号される可能性がある課題があった。

【0069】本発明はこのような状況に鑑みてなされたものであり、秘密裡に保管しておくべき情報が露呈した装置に対してデータの伝送を行わないようにし、より安全性を図るようにするものである。

【0070】

【課題を解決するための手段】請求項1に記載の情報処

理装置は、他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成手段と、作成手段により作成されたリストを、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供する提供手段とを備えることを特徴とする。

【0071】請求項4に記載の情報処理方法は、他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成ステップと、作成ステップで作成されたリストを、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供する提供ステップとを備えることを特徴とする。

【0072】請求項5に記載の提供媒体は、他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成ステップと、作成ステップで作成されたリストを、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供する提供ステップとを有するコンピュータプログラムを提供することを特徴とする。

【0073】請求項6に記載の情報処理装置は、他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信手段と、受信手段により受信されたリストに記されている識別番号と、記憶手段により記憶された識別番号テーブル中の識別番号とを比較する比較手段と、比較手段による比較結果に対応して、暗号化データを他の情報処理装置に伝送する伝送手段とを備えることを特徴とする。

【0074】請求項13に記載の情報処理方法は、他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶ステップと、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信ステップと、受信ステップで受信されたリストに記されている識別番号と、記憶ステップで記憶された識別番号テーブル中の識別番号とを比較する比較ステップと、比較ステップにおける比較結果に対応して、暗号化データを他の情報処理装置に伝送する伝送ステップとを備えることを特徴とする。

【0075】請求項14に記載の提供媒体は、他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶ステップと、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信ステップと、受信ステップで受信されたリストに記されている識別番号と、記憶ステップで記憶された識別番号テーブル中の識別番号とを比較する比較ステップと、比較ステップにおける比較結果に対応して、暗号化データを他の情報処理装置に伝送する伝送ステップと

を有するコンピュータプログラムを提供することを特徴とする。

【0076】請求項15に記載の情報処理システムは、第1の情報処理装置が、秘密裡にしておくべき情報が露呈された第3の情報処理装置の識別番号を示したリストを作成する作成手段と、作成手段により作成されたリストを第2の情報処理装置に提供する提供手段とを備え、第2の情報処理装置が、バスを介して接続されている第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段と、第1の情報処理装置の提供手段により提供されたリストを受信する受信手段と、受信手段により受信されたリストに示されている識別番号と、記憶手段により記憶された識別番号テーブル中の識別番号とを比較する比較手段と、比較手段による比較結果に対応して、第3の情報処理装置に暗号化データを伝送する伝送手段とを備えることを特徴とする。

【0077】請求項16に記載の情報処理方法は、第1の情報処理装置が、秘密裡にしておくべき情報が露呈された第3の情報処理装置の識別番号を示したリストを作成する作成ステップと、作成ステップで作成されたリストを第2の情報処理装置に提供する提供ステップとを備え、第2の情報処理装置が、バスを介して接続されている第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶ステップと、第1の情報処理装置の提供ステップにおいて提供されたリストを受信する受信ステップと、受信ステップで受信されたリストに示されている識別番号と、記憶ステップで記憶された識別番号テーブル中の識別番号とを比較する比較ステップと、比較ステップにおける比較結果に対応して、第3の情報処理装置に暗号化データを伝送する伝送ステップとを備えることを特徴とする。

【0078】請求項17に記載の提供媒体は、秘密裡にしておくべき情報が露呈された第3の情報処理装置の識別番号を示したリストを作成する作成ステップと、作成ステップで作成されたリストを第2の情報処理装置に提供する提供ステップとを有する、第1の情報処理装置に用いられるコンピュータプログラムと、バスを介して接続されている第3の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶ステップと、第1の情報処理装置の提供ステップにおいて提供されたリストを受信する受信ステップと、受信ステップで受信されたリストに示されている識別番号と、記憶ステップで記憶された識別番号テーブル中の識別番号とを比較する比較ステップと、比較ステップにおける比較結果に対応して、第3の情報処理装置に暗号化データを伝送する伝送ステップとを有する、第2の情報処理装置に用いられるコンピュータプログラムとを提供することを特徴とする。

【0079】請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体においては、他の情報処理装置のうち、秘密裡に保管

しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストが作成され、作成されたリストが、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供される。

【0080】請求項6に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項14に記載の提供媒体においては、他の情報処理装置の識別番号が識別番号テーブルとして記憶され、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストが受信され、受信されたリストに記されている識別番号と、識別番号テーブル中の識別番号とが比較され、比較結果に対応して、暗号化データが他の情報処理装置に伝送される。

【0081】請求項15に記載の情報処理システム、請求項16に記載の情報処理方法、および請求項17に記載の提供媒体においては、第1の情報処理装置において、秘密裡にしておくべき情報が露呈された第3の情報処理装置の識別番号を示したリストが作成され、作成されたリストが第2の情報処理装置に提供され、第2の情報処理装置において、バスを介して接続されている第3の情報処理装置の識別番号が識別番号テーブルとして記憶され、第1の情報処理装置から提供されたリストが受信され、受信されたリストに示されている識別番号と、識別番号テーブル中の識別番号とが比較され、その比較結果に対応して、第3の情報処理装置に暗号化データが伝送される。

【0082】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を附加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0083】請求項1に記載の情報処理装置は、他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成する作成手段（例えば、図1のリボケーションリスト作成部111）と、作成手段により作成されたリストを、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供する提供手段（例えば、図1の送信部112）とを備えることを特徴とする。

【0084】請求項2に記載の情報処理装置は、作成主により作成されたリストに、自分自身のデジタル署名を付加する付加手段（例えば、図1のリボケーションリスト作成部111）をさらに備えることを特徴とする。

【0085】請求項6に記載の情報処理装置は、他の情報処理装置の識別番号を識別番号テーブルとして記憶する記憶手段（例えば、図1のEEPROM134）と、秘密裡

に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信する受信手段（例えば、図1のチューナ132）と、受信手段により受信されたリストに記されている識別番号と、記憶手段により記憶された識別番号テーブル中の識別番号とを比較する比較手段（例えば、図5のステップS207）と、比較手段による比較結果に対応して、暗号化データを他の情報処理装置に伝送する伝送手段（例えば、図1の1394インターフェース138）とを備えることを特徴とする。

【0086】請求項8に記載の情報処理装置は、リストに付加されている署名を用いて、リストが正規のものであるか否かを検証する検証手段（例えば、図5のステップS205）をさらに備えることを特徴とする。

【0087】請求項9に記載の情報処理装置は、比較手段の比較の結果、リスト中の識別番号と合致する識別番号が識別番号テーブルに存在した場合、識別番号テーブル中の、対応する識別番号にフラグを付加する付加手段（例えば、図5のステップS209）をさらに備えることを特徴とする。

【0088】図1は、本発明を適用した情報処理システムの構成例を示す図であり、図9に示した場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する。この構成例においては、管理センタ110は、不正装置の識別番号が記載されたリスト（revocation list：リボケーションリスト）を作成するリボケーションリスト作成部111と、リボケーションリスト作成部111により作成されたリボケーションリストをアンテナ113を介して送信する送信部112とにより構成されている。

【0089】リボケーションリスト作成部111は、所定の装置において管理されている情報の露呈が発覚した場合、その装置の識別番号（device_ID）を不正装置のdevice_IDとして記したリスト（以下、リボケーションリスト（revocation list）と称する）を作成する。また、リボケーションリスト作成部111は、リボケーションリストを作成したものが管理センタ110であることを示す署名（例えば、公開鍵暗号を用いたデジタル署名）とその作成時刻を、作成したリボケーションリストに付加する。このデジタル署名は、リボケーションリストを受け取った装置において、そのリボケーションリストが正規のものであるのか否かの検証の際に用いられる。送信部112は、所定のタイミングで、リボケーションリスト作成部111により作成されたリボケーションリストを、アンテナ113を介して送信する。なお、このタイミングは、例えば、1ヶ月に一度の定期的なものでもよいし、例えば、また、他の装置から要求があったときのタイミングでもよい。

【0090】管理センタ110から送信されたリボケーションリストは、例えば衛星120を介して、他の装置（いまの場合、データ放送受信装置130）に提供され

る。

【0091】データ放送受信装置130は、1394インターフェース138を介して1394バス11に接続されている。チューナ132は、アンテナ131を介して、管理センタ110から衛星120を介して送信されるリボケーションリストを受信し、CPU133に出力するようになされている。CPU133は、ROM136に記憶されているプログラムに従って各種の処理を実行し、RAM137は、CPU133が各種の処理を実行する上において必要なデータやプログラム等を適宜記憶する。ハードディスク(HDD)135は、データまたはプログラムなどを記録または再生することができるようになされている。EEPROM134は、装置の電源オフ後も記憶する必要のある情報(例えば、リボケーションリスト)を記憶するようになされている。内部バス139は、これらの各部を相互に接続している。

【0092】なお、DVDプレーヤ1、パーソナルコンピュータ2、および光磁気ディスク装置3の詳細な構成は、図10に示した場合と同様とされている。

【0093】ここで、1394バス11に接続されている各装置には、それぞれに固有の識別番号であるdevice_ID(例えば、node_unique_ID)が与えられている。また、各装置のうち、データ放送受信装置130、DVDプレーヤ1、パーソナルコンピュータ2、または光磁気ディスク3等の、他の装置間でデータを送受信することができる装置(以下、特にこれらの装置を個々に区別する必要がない場合、適宜、これらの装置を総称して送受信装置と記述する)は、1394バス11を介して自分に接続されている装置(具体的には、少なくとも一度、データの伝送を行った相手の装置)のdevice_IDが記される識別番号テーブル(connected device_ID table:以下、CDTと略記する)を、例えば、それぞれに内蔵するEEPROM内(例えば、データ放送受信装置の場合、EEPROM134内)の所定の領域に用意している。なお、各装置のうち、データの送信を行うことができない装置は、CDTを有する必要はない。

【0094】各送受信装置は、例えば、図8を参照して後述する認証処理(勿論、これ以外の認証処理でもよい)を行う際に、相手装置のdevice_ID入手し、それをCDTに格納することができる。そして、各送受信装置は、相手側のdevice_IDを確認した後(すなわち、相手装置が正当な装置であるか否かを確認した後)、暗号化データを復号するための鍵(例えば、セッションキーまたは時変キー)を相手装置に送信するか否かを決定するようになされている。

【0095】データ放送受信装置130は、1394バス11に接続されているこれらの全装置のdevice_IDまたは各送受信装置のCDTに格納されている情報を、所定のタイミングで適宜読み出すことができるようになされている。このタイミングは、例えば、一週間に一回のよう

に、定期的なものであってもよいし、また、例えば、1394バス11に新たな装置が追加または排除されたことが検出できる場合、それが検出されたタイミングで行うよいにしてもよい。そして、データ放送受信装置130は、読みとった情報を自己自身のCDTに反映する(具体的には、新規の項目を格納する)ことができる。

【0096】図2は、CDTの構成例を示す図である。この例において、アドレス1乃至nには、1394バス11を介して接続されている装置のdevice_IDと、不正装置のdevice_ID(リボケーションリストに記されているdevice_ID)であるか否かを示すフラグ(revokeフラグ)とが格納されるようになされている。この例においては、アドレス1乃至3のdevice_IDA乃至device_IDCに、フラグ(×印)が付加されている(具体的には、フラグを示す値が、例えば1に設定されている)。すなわち、これらのdevice_IDA乃至device_IDCに対応する装置は、不正な装置であるとされる。

【0097】データ放送受信装置130(または他の送受信装置)は、フラグが格納されているdevice_ID(すなわち、不正装置に対応するdevice_ID)が、常にアドレスの前段に配置されるように、CDTをソートするようになされている。例えば、図3に示すように、アドレス6に格納されているdevice_IDFに対応する装置が不正装置であることが新たに発覚し、そのアドレス6にフラグが付加されたとき、データ放送受信装置130のCPU133は、図4に示すように、アドレス6に格納されていたdevice_IDFを、アドレス4に移動させるとともに、アドレス4とアドレス5に格納されていたdevice_IDEとdevice_IDFを、それぞれアドレス5とアドレス6に移動させる。

【0098】なお、CDTには、n個(例えば、100個)の項目(device_IDとフラグ)を格納することができるものとする。ただし、各送受信装置のうち、管理センタ110から提供されるリボケーションリストを用いて、各装置のdevice_IDまたはCDTを管理する管理装置(いまの場合、データ放送受信装置130)のCDTには、n個以上のdevice_IDとフラグを格納することができるものとする。ここで、このCDTのアドレスが全て使用されている状態において、新たにCDTに格納すべき項目が発生した場合、CDT中の、フラグが付加されていない項目のうち、一番古いものが消去され、空いたアドレスに新規の項目が格納される。

【0099】例えば、いま、100個の項目を格納することができるCDTがあり、そのアドレス1乃至アドレス10までは、フラグが付加されている項目が、古いものから順に格納されており、また、そのアドレス11乃至アドレス100までは、フラグが付加されていない項目が、古いものから順に格納されているものとする。例えば、このCDTを有する装置が、データの伝送を初めて行う相手装置のdevice_ID入手し、これを新たな項目と

してCDTに格納する場合、フラグが付加されていない項目のうち、一番古いものである、アドレス11の項目を消去し、アドレス12乃至アドレス100に格納されていった項目を1つずつ繰り上げる（それぞれアドレス11乃至99に移動する）。そして、それにより空いたアドレス100に、新たな項目が格納される。

【0100】また、例えば、このCDTを持つ装置が、新たにリボケーションリストを受け取り、その中のdevice_IDをCDTに格納する場合、アドレス11の項目を消去して、そこに、リボケーションリストのdevice_IDを、フラグとともに格納する。

【0101】さらに、このCDTが、フラグが付加されている項目で一杯となった場合において、このCDTを有する装置は、新規に格納すべき項目が、新たに受け取ったリボケーションリストのdevice_IDであるとき、CDTの古い項目を消去して、空いたアドレスに格納し、データの伝送を初めて行った相手装置のdevice_IDであるとき、それはCDTに格納しない。

【0102】次に、図5のフローチャートを参照して、図1の情報処理システムの動作を説明する。ステップS201において、管理センタ110のリボケーション作成部111は、不正装置のdevice_IDを示したリボケーションリストを作成し、続いて、ステップS202において、作成したリボケーションリストに、署名と時刻を付加する。ステップS203で、送信部112は、所定のタイミングで、リボケーション作成部111により作成されたリボケーションリストを、アンテナ113を介して送信する。

【0103】そして、ステップS204において、データ放送受信装置130のチューナ132は、衛星120を介して提供されるリボケーションリストを、アンテナ131を介して受信する。CPU133は、ステップS205において、受信したリボケーションリストが、正当なものであるか否かを検証する。すなわち、リボケーションリストに付加されている署名が、管理センタ110のものであるかを検証する。なお、この検証処理においては、例えば、管理センタ110から発行された公開鍵を有する装置のみが署名を確認することができるものとする。

【0104】ステップS205において、リボケーションリストが正当なものではない（すなわち、署名が管理センタ110のものではない）と判定された場合、CPU133は、ステップS206においてリボケーションリストは不正なものとして破棄し、処理を終了する。一方、ステップS205において、リボケーションリストが正当なものである（すなわち、署名が管理センタ110のものである）と判定された場合、ステップS207に進み、CPU133は、リボケーションリスト中に記されている不正装置のdevice_IDと、CDT中のdevice_IDとを比較する。CPU133は、ステップS208において

て、CDT中に、リボケーションリストに記されているdevice_IDと合致するdevice_IDが存在するか否かを判定し、対応するdevice_IDはCDT中に存在しないと判定した場合、処理を終了する。

【0105】ステップS208において、リボケーションリストに記されているdevice_IDと合致するdevice_IDがCDT中に存在すると判定された場合、ステップS209に進み、CPU133は、CDT中の対応するdevice_IDにフラグを付加する。続いて、CPU133は、ステップS210において、1394インターフェース138を制御して、CDT中の、フラグが付加されているdevice_IDを、リボケーションリストとともに、1394バス11を介して接続されている他の送受信装置に送信する。

【0106】各送受信装置は、ステップS211において、データ放送受信装置130のフラグが付加されたdevice_IDとリボケーションリストを受信し、ステップS212において、受信したリボケーションリストが正当なものであるか否かを判定する。ステップS212において、リボケーションリストは正当なものではない（すなわち、署名が管理センタ110のものではない）と判定された場合、ステップS213において、そのリボケーションリストが破棄され、処理が終了される。

【0107】ステップS212において、リボケーションリストが正当なものであると判定された場合、ステップS214に進み、各送受信装置は、受信したリボケーションリストに対応して、それぞれのCDTの内容を更新する（対応するdevice_IDにフラグを付加する）。

【0108】以上の処理により、1394バス11に接続されている全ての送受信装置のCDTが、管理センタ110により作成されたリボケーションリストに対応して更新された。

【0109】次に、以上をふまえた上で、図7を参照して、例えば、送受信装置としてのDVDプレーヤ1に対して、パーソナルコンピュータ2からデータの伝送の要求があった場合の、DVDプレーヤ1の処理を説明する。まず、ステップS301において、DVDプレーヤ1は、パーソナルコンピュータ2との間で認証処理（例えば、図8を用いて後述）を実行する。これにより、DVDプレーヤ1は、パーソナルコンピュータ2のdevice_IDを入手することになる。ステップS302において、パーソナルコンピュータ2のdevice_IDが、自分自身のCDT中でフラグが付加されているdevice_IDであるか否かが判定され、パーソナルコンピュータ2のdevice_IDが、CDT中でフラグが付加されているものであると判定された場合、ステップS303において、DVDプレーヤ1は、パーソナルコンピュータ2を不正装置であるとし、処理を終了する。

【0110】ステップS302において、パーソナルコンピュータ2のdevice_IDは、CDT中でフラグが付加されているものではないと判定された場合、ステップS30

4に進み、DVDプレーヤ1は、パーソナルコンピュータ2との間で、鍵および暗号データの伝送処理を実行する。続いて、ステップS305において、DVDプレーヤ1は、パーソナルコンピュータ2が、新規の装置であるか（すなわち、伝送処理を初めて行った装置であるか）否かを判定し、パーソナルコンピュータ2は新規の装置ではない（すなわち、伝送処理を既に行ったことがある装置である）と判定した場合、処理を終了する。

【0111】ステップS305において、パーソナルコンピュータ2が新規の装置である（すなわち、初めて伝送処理を行った装置である）と判定された場合、ステップS306に進み、DVDプレーヤ1は、パーソナルコンピュータ2のdevice_IDをCDTに追加する。これにより、データ放送受信装置130は、DVDプレーヤ1のCDTを所定のタイミングで読み出したときに、1394バス11に新規に接続された装置（いまの場合、パーソナルコンピュータ2）のdevice_IDを入手することできるので、例えば、次に受け取ったリボケーションリストにより、このパーソナルコンピュータ2が不正装置であることが判明した場合、1394バス11に接続されている各送受信装置（パーソナルコンピュータ2を除く）にこれを知らせることにより、パーソナルコンピュータ2を実質的に排除することが可能となる。

【0112】以上のようにして、各送受信装置は、管理センタ110から提供されたリボケーションリストに対応して、相手装置が不正な装置であるか否かを判断することができ、映画などのデータの伝送を安全に行うことができる。

【0113】図8は、図7のステップS301で実行される認証の処理例を示すタイミングチャートである。この例においては、ソースとしてのDVDプレーヤ1のEEPROM27には、サービスキー(service_key)とhash関数(F, G, H)が予め記憶されている。一方、シンクとしてのパーソナルコンピュータ2は、そのdevice_ID(ID)、ライセンスキー(license_key)、および、hash関数(G, H)を、EEPROM50に秘密裡に保持している。まず、ステップS111において、パーソナルコンピュータ2は、乱数Nbを生成する。そして、ステップS112において、1394インターフェース49を制御して、生成した乱数Nbとともに認証要求を1394バス11を介してDVDプレーヤ1に送信する。

【0114】DVDプレーヤ1は、ステップS113において、この認証要求と乱数Nbを受信する。次にDVDプレーヤ1は、ステップS114において、パーソナルコンピュータ2に対してそのdevice_IDを要求する。パーソナルコンピュータ2は、ステップS115において、device_IDの要求を受信し、その対応として、ステップS116において、EEPROM50に記録されているdevice_IDを読み出し、それをDVDプレーヤ1に送信する。これにより、DVDプレーヤ1は、パーソナルコンピュータ2

のdevice_IDを入手することができる。

【0115】DVDプレーヤ1は、ステップS117において、パーソナルコンピュータ2から送信されたdevice_IDを受信し、ステップS118において、次式で示すように、サービスキー(Kser)を鍵とするhash関数Fに、受信したIDを適用することにより、データKvを生成する。なお、keyedhashA1(A2, A3)は、A2を鍵とするhash関数A1に、A3を適用することを示している。

10 Kv=keyedhashF(Kser, ID)

【0116】次に、DVDプレーヤ1は、ステップS119で、乱数Naを生成し、ステップS120で、乱数Naをパーソナルコンピュータ2に送信する。パーソナルコンピュータ2は、ステップS121で乱数Naを受信し、ステップS122において、次式に示すように、ライセンスキーKlicを鍵とするhash関数Hに、乱数Naと乱数Nbを連結したデータ(Na||Nb)を適用することにより、データRを生成する。

R=keyedhashH(Klic, Na||Nb)

20 20 【0117】そして、パーソナルコンピュータ2は、ステップS123において、生成したデータRをDVDプレーヤ1に送信する。DVDプレーヤ1は、ステップS124で、データRを受信し、ステップS125において、ステップS118で生成されたデータKvを鍵とするhash関数Hに連結データ(Na||Nb)を適用して得られた値が、受信されたデータRと等しいか否かを判定する。

【0118】ステップS125において、両者が等しくないと判定された場合、受信されたデータRは破棄され、認証処理は終了される（すなわち、パーソナルコンピュ

30 テータ2は不適正なものと判定される）。一方、ステップS125において、両者が等しいと判定された場合、ステップS126に進み、DVDプレーヤ1は、次式に示すように、データKvを鍵とするhash関数Gに連結データ(Na||Nb)を適用することにより、鍵Kabを生成する。

Kab=keyedhashG(Kv, Na||Nb)

【0119】なお、この鍵Kabは、DVDプレーヤ1とパーソナルコンピュータ2の間で一時的に用いられる鍵である。例えば、ソースとしてのDVDプレーヤ1に、パーソナルコンピュータ2の他にシンクとして光磁気ディスク

40 装置3が接続されている場合、DVDプレーヤ1と光磁気ディスク装置3との間で用いられる鍵が、さらに別途生成されることになる。

【0120】次に、ステップS127において、DVDプレーヤ1は、セッション内で共通に使用する鍵Kcを生成し、ステップS128において、鍵Kabを用いて鍵Kcを暗号化して、暗号化データ（暗号化鍵）Xを生成する。すなわち、次式が演算される。なお、Enc(B1, B2)は、B1を鍵として、B2を暗号化することを示している。

X=Enc(Kab, Kc)

【0121】そして、DVDプレーヤ1は、ステップS129において、暗号化データXをパソコンコンピュータ2に送信する。ステップS130において、パソコンコンピュータ2は、DVDプレーヤ1から送信された暗号化データXを受信し、ステップS131で、ライセンスキーキーKlicを鍵とするhash関数Gに、連結データ(Na||Nb)を適用することにより、鍵K'abを生成する。すなわち、次式が演算される。

$$K'ab = \text{keyedhashG}(Klic, Na || Nb)$$

【0122】そして、ステップS131において、パソコンコンピュータ2は、次式に示すように、鍵K'abを用いてデータXを復号して、鍵Kcを得る。なお、Dec(C1, C2)は、C1を鍵として、C2を復号することを示している。

$$Kc = \text{Dec}(K'ab, X)$$

【0123】これにより、例えば、シンクとしての装置が複数存在する場合においても、ソースと全てのシンクとの間で、同一の鍵Kcを安全に共有することができる。

【0124】そして、DVDプレーヤ1のファームウェア20は、ステップS121において、乱数N'aを生成し、ステップS133において、乱数N'aをパソコンコンピュータ2に送信する。パソコンコンピュータ2のライセンスマネージャ62は、ステップS134で、乱数N'aを受信する。そして、DVDプレーヤ1のファームウェア20とパソコンコンピュータ2のライセンスマネージャ62は、それぞれ、ステップS135とステップS136において、鍵Kcと乱数N'aを用いて次式を演算することにより、ともにセッションキー-skを得る。

$$sk = \text{keyedhashH}(Kc, N'a)$$

【0125】なお、セッションキーを変更する場合、ソースは、新たな乱数を生成して、シンクとなる全ての装置にそれを送信し、それぞれの装置において、その新たな乱数を用いてセッションキーを生成するようとする。

【0126】ところで、以上の処理では、各送受信装置が、リボケーションリストの正当性を確認することができるようになるため、管理装置であるデータ放送受信装置130は、受信したリボケーションリストを各送受信装置に伝送するようになされているが、リボケーションリストのデータサイズが大きい場合、通信コストが高くなることが予想される。そこで、この対策として、以下の2つの方法が考えられる。

(1) 管理センタ110が、リボケーションリストを作成する際に、それを所定の数に分割し、分割したリストそれぞれに対して署名を付加し、それをデータ放送受信装置130等の管理装置に提供し、また、データ放送受信装置130等の管理装置は、管理センタ110から提供されたリボケーションリストの中から、自分自身に接続されている装置に関連するものだけを、接続されている他の送受信装置に伝送するようとする。

(2) データ放送受信装置130等の管理装置は、デ

ジタル署名を作成する機能を備えるようにし、リボケーションリストの中から自分のCDTに含まれている部分を取り出し、自分のネットワーク用のリボケーションリストを新たに作成して、それに署名を付加し、それを接続されている他の送受信装置に伝送するようとする。

【0127】なお、上記の各種の指令を実行するプログラムまたはリボケーションリストは、磁気ディスク、CD-ROM等の伝送媒体を介してユーザに提供したり、ネットワーク等の伝送媒体を介してユーザに提供し、必要に応じて内蔵するRAMやハードディスク等に記憶して利用させようすることができる。

【0128】

【発明の効果】以上のように、請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体によれば、他の情報処理装置のうち、秘密裡に保管しておくべき情報が露呈された第1の情報処理装置の識別番号が記されたリストを作成し、作成されたリストを、他の情報処理装置のうち、第1の情報処理装置以外の第2の情報処理装置に提供するようにしたので、秘密裡に保管しておくべき情報が露呈した装置のdevice_IDを、他の装置に知らせることができる。

【0129】請求項6に記載の情報処理装置、請求項13に記載の情報処理方法、および請求項14に記載の提供媒体によれば、他の情報処理装置の識別番号を識別番号テーブルとして記憶し、秘密裡に保管しておくべき情報が露呈された情報処理装置の識別番号が記されたリストを受信し、受信されたリストに記されている識別番号と、識別番号テーブル中の識別番号とを比較し、その比較結果に対応して、暗号化データを他の情報処理装置に伝送するようにしたので、秘密裡に保管しておくべき情報が露呈した装置に対して、データの伝送を行わないようすることができる。

【0130】請求項15に記載の情報処理システム、請求項16に記載の情報処理方法、および請求項17に記載の提供媒体によれば、第1の情報処理装置は、秘密裡にしておくべき情報が露呈された第3の情報処理装置の識別番号を示したリストを作成し、作成されたリストを第2の情報処理装置に提供し、第2の情報処理装置は、バスを介して接続されている第3の情報処理装置の識別

番号を識別番号テーブルとして記憶し、第1の情報処理装置から提供されたリストを受信し、受信されたリストに示されている識別番号と、識別番号テーブル中の識別番号とを比較し、その比較結果に対応して、第3の情報処理装置に暗号化データを伝送するようにしたので、秘密裡に保管しておくべき情報が露呈した装置に対してデータの伝送を行わないようにし、より安全性を図ることができる。

【図面の簡単な説明】

【図1】本発明を適用した情報処理システムの構成例を示すブロック図である。

【図2】CDTの構成例を示す図である。

【図3】図2のCDTに新規のdevice_IDが追加された様子を示す図である。

【図4】CDTのアドレスをソートする処理を説明する図である。

【図5】図1の情報処理システムの処理を説明するフローチャートである。

【図6】図5に続く図である。

【図7】DVDプレーヤー1の処理を説明するフローチャートである。

【図8】図7のステップS301の認証処理を説明するタイミングチャートである。

【図9】従来の情報処理システムの構成例を示すブロック図である。

【図10】図8のDVDプレーヤ1、パソコンコンピュータ2、および光磁気ディスク装置3の内部の構成例を示すブロック図である。

【図11】認証処理を説明する図である。 4 EEPROM, 135 ハードディスク, 136 RO
【図12】認証処理を説明するタイミングチャートである M, 137 RAM, 138 1394インターフェース,

【図13】node_unique_IDのフォーマットを示す図である。

* る。

【図14】他の認証処理を説明するタイミングチャートである。

【図15】他の認証処理を説明するタイミングチャートである。

【図16】他の認証処理を説明するタイミングチャートである。

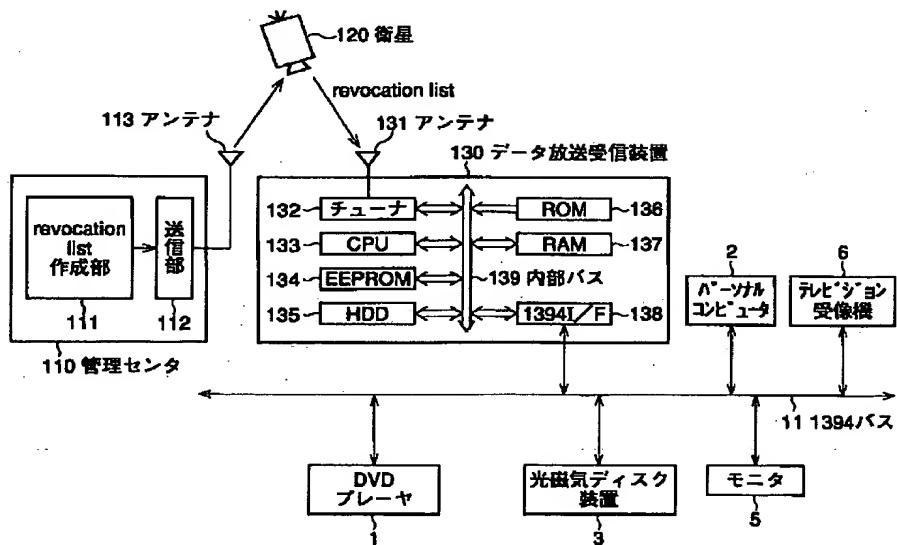
【図17】他の認証処理を説明するタイミングチャートである。

10 【図18】暗号化処理を説明するブロック図である。

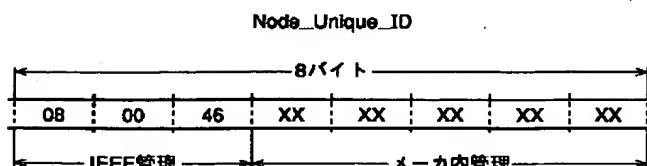
【符号の説明】

- 1 DVDプレーヤ, 2 パーソナルコンピュータ,
 3 光磁気ディスク装置, 11 1394バス, 110
 管理センタ, 111 リポケーションリスト作成
 部, 112 チューナ, 113 アンテナ, 12
 0 衛星, 130 データ放送受信装置, 131
 アンテナ, 132 チューナ, 133 CPU, 13
 4 EEPROM, 135 ハードディスク, 136 R0
 M, 137 RAM, 138 1394インターフェース,
 139 内部バス

[図 1]



【図 1-3】



【図2】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	D	
5	E	
6		
.		
.		
.		
n		

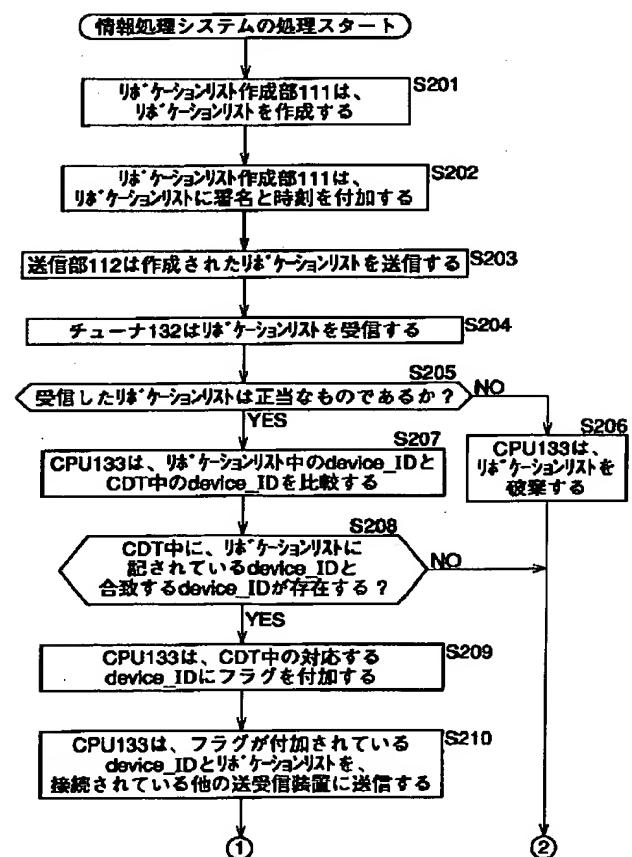
【図3】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	D	
5	E	
6	F	X (新規)
.		
.		
.		
n		

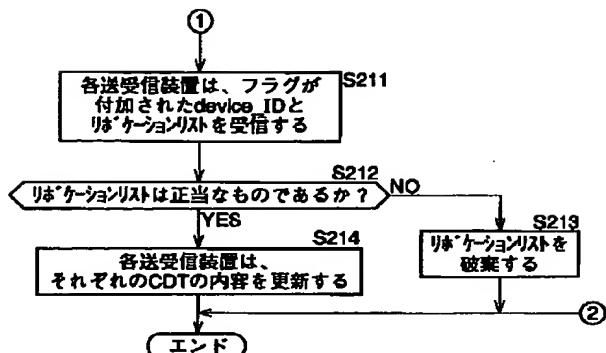
【図4】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	F	X
5	D	
6	E	
.		
.		
.		
n		

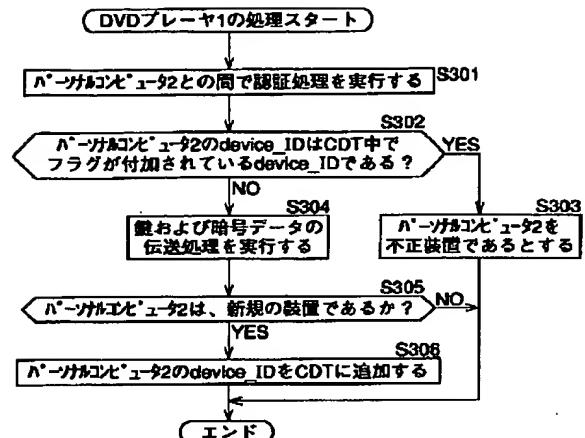
【図5】



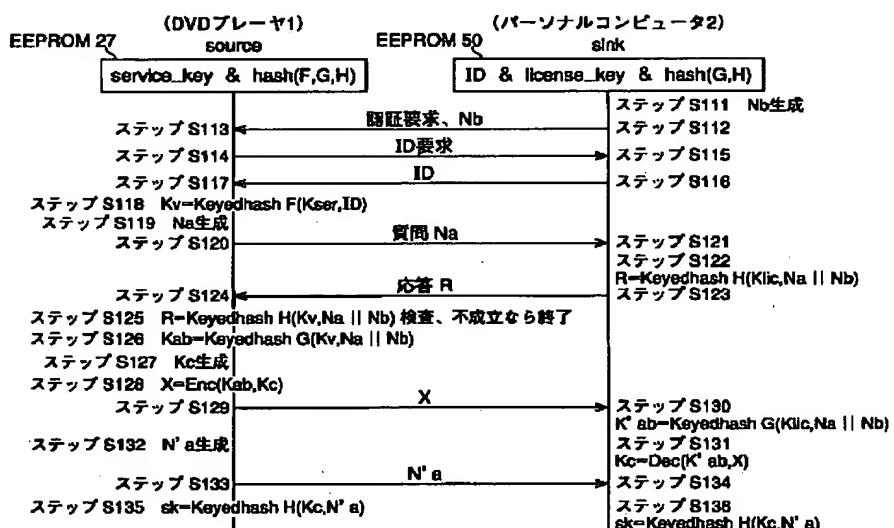
【図6】



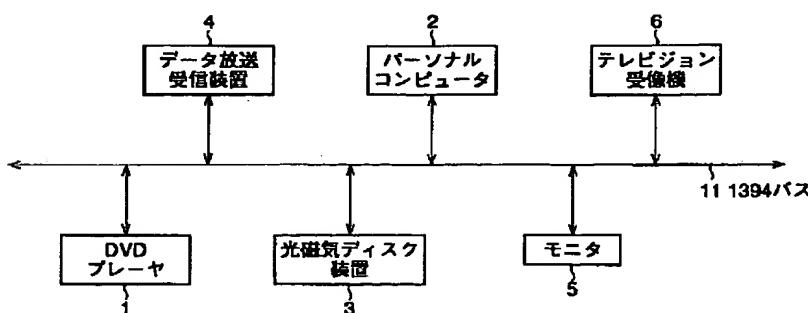
【図7】



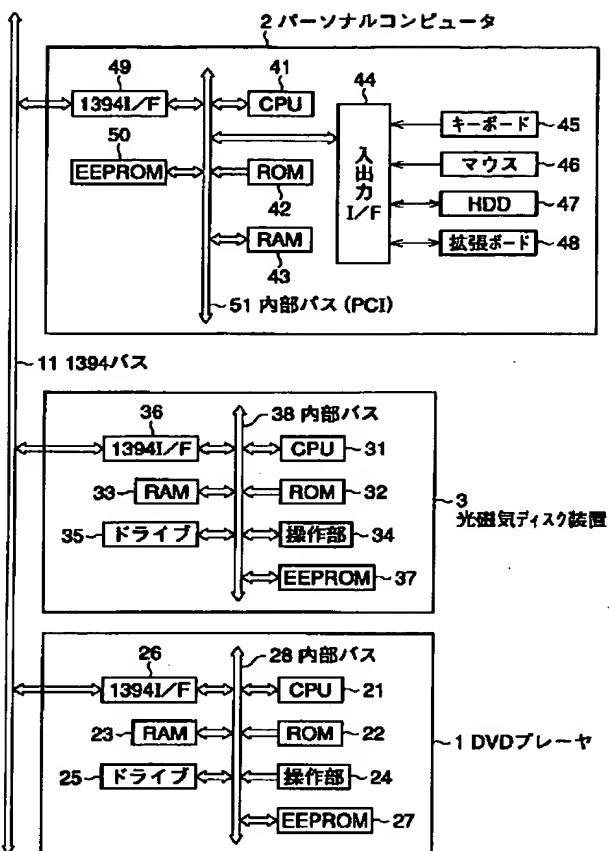
【図8】



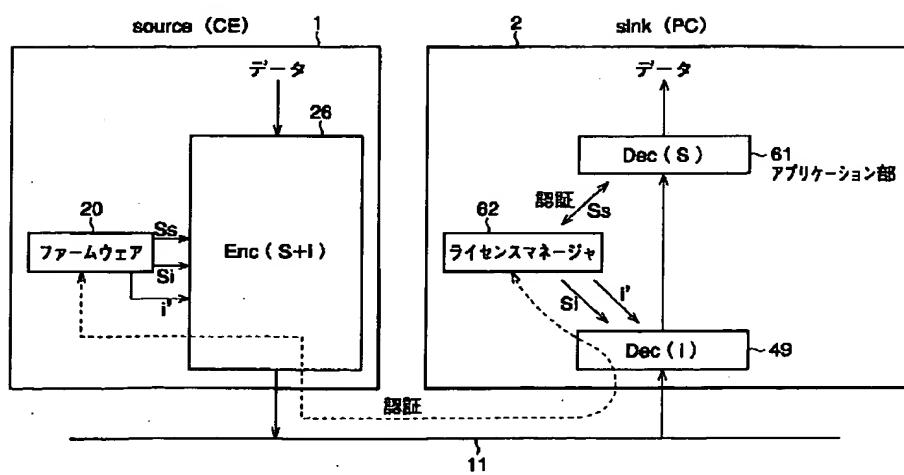
【図9】



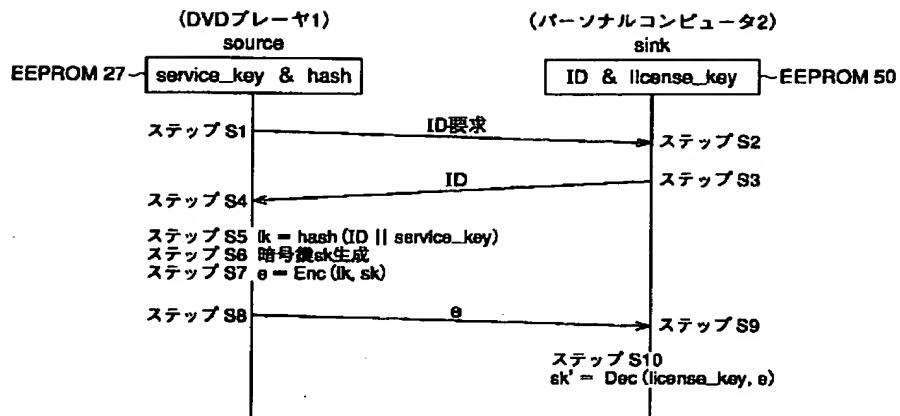
【図 10】



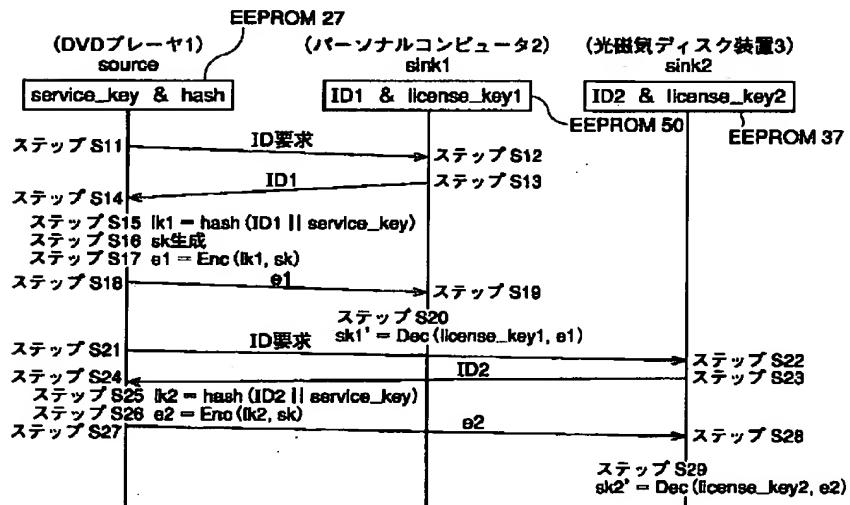
【図 11】



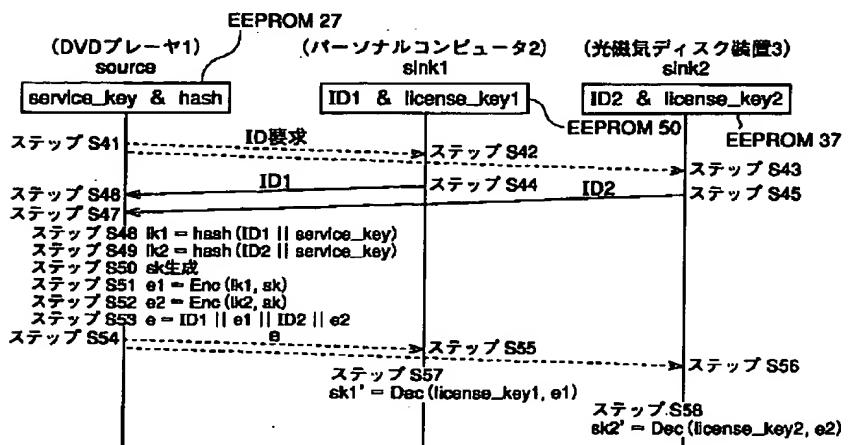
【図12】



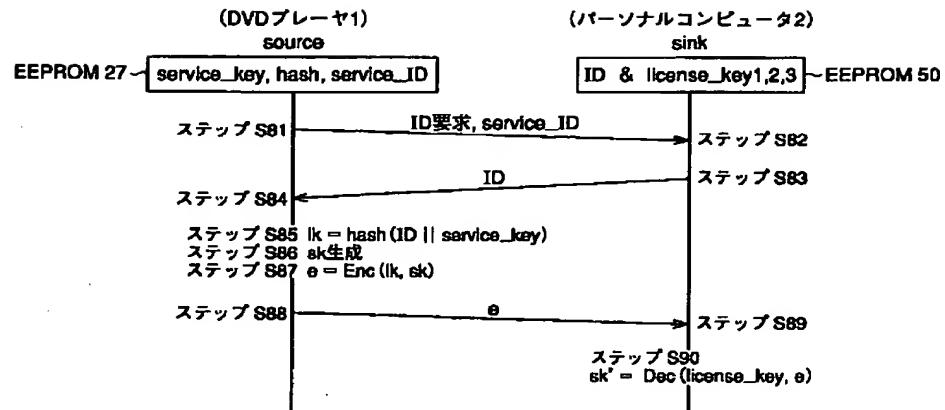
【図14】



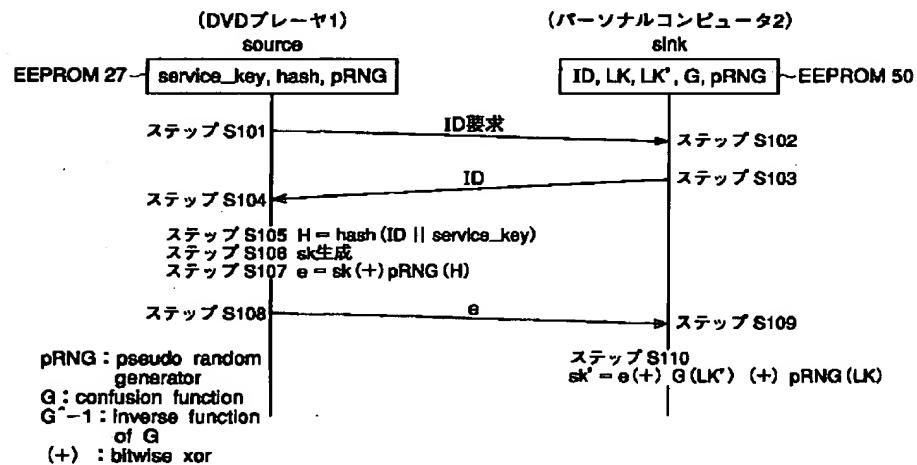
【図15】



【図16】



【図17】



【図18】

